EXHIBIT 83

What do we need to know about Chrome Incognito mode to improve it?

Author: rhalavati@

Status: Final, please see go/chrome_incognito_short_term for follow up.

Last Update: 2018-09-24

Introduction

There is a gap between our promises about Chrome Incognito mode, their delivery, and user expectations. This is partly because of not being able to transfer the message to the users, and partly due to missing/incomplete features.

There are different possibilities on how to reduce the gap, but to proceed we need to know what are the communication problems regarding incognito mode, and what are the actual additional required features. The goal of this document is to prepare a list of questions as a basis for a user study on this issue.

What do we know about user expectations?

There have been previous internal and external studies on user expectations from a private/incognito mode, such as [1] and [2] internally and [3] and [4] externally. Here is a list of mentioned expectations:

- Prevention of browsing traces locally.
- Hiding activities such as browsing adult content, health content, gift shopping, price comparison, and content not safe for work.

[1] Perceptions Of Chrome Incognito (2015) (go/percep-incognito)
[2] Exploration of primary value proposition of Incognito to users (go/incognito-pvp-qcs)
[3] "Your Secrets Are Safe: How Browsers' Explanations Impact Misconceptions About Private Browsing Mode", Wu et al., Proceedings of the 2018 World Wide Web Conference.
[4] "Away From Prying Eyes: Analyzing Usage and Understanding of Private Browsing", Habib et al., Proceedings of the 14th Symposium on Usable Privacy and Security, Aug 2018, Baltimore, US.

Commented [1]: Would be particularly curious how this varies by form factor (desktop v mobile), by country, and potentially by gender. For reference, we see a lot of casual sharing of mobile devices in NBU. As a result, people are often very worried about they privacy of their browser behavior from the people around them (more so than from Google or websites)

Commented [2]: (Moved the content and your comment.)

Commented [3]: from ___ ? Family/friends who have access to device, or ISPs / government / external observers?

- Bypassing customization (such as search autocomplete).
- Avoiding automatic login and storage of login information.
- Hiding search/browsing activity from Google/websites.
- Anonymity (not being identified by the websites).
- Faster browsing by disabling extensions and plugins.
- Management of re-identifying cookies.
- Avoid being tracked by websites (targeted ads).
- Storing too many cookies or history entries.
- Accommodate intentional or unintentional use by others.
- Location hiding.

As summarized in [5], the major misconceptions are around the following:

- Incognito browsing is visible by the network and is not necessarily secure.
- Incognito browsing is prone to fingerprinting and IP addresses are not hidden.
- Incognito mode does not block ads.
- Browsing and search will be remembered by the websites.
- If logged in from inside incognito mode, all activities in the website (and related websites) will be remembered.

These misconceptions may come from incognito brand name, icon, and the limited incognito education in the incognito NTP message.

General Questions

Category Zero: Privacy in General

1. How would users feel about a browser that proactively helped them to better understand and protect their privacy?
2. How significant would they rate the above feature (in contrast to other decision factors) when choosing a browser for the first time and when switching to another browser?

[5] Five Ways People Misunderstand Incognito & Private Browsing (2018) (go/five-misunderstandings-incognito)

3. Would they prefer this to be an invisible feature (silently protecting them) or one that is more visible and educating in nature?
4. Do users want to be educated by the software, and how?
5. Does having a distinguishable theme for incognito/private mode helps users by making less mistake in differentiating them, or they feel uncomfortable when other see them use the private/incognito mode?

Category one: The message

In one previous study (go/reimagining-incognito-research) we have found that incognito icon alone does not transfer that much meaning to the users and changing it did not have significant (positive) effect on correct conceptions.

Another study (go/incognito-pvp-gcs) on difference of the words 'incognito' and 'private' showed that 'private' has more alignment with incognito principles and the word 'incognito' has a vague meaning to the users. This study has been done on american users and it may have different results for non-English speaking users or less educated users.

incognito	private
	

It is nice to know is

1. Is it better to have a more clear brand name or a rather vague name ('incognito').
    a. Does a more clear name result in more "correct" usage?
    b. Does a more clear name result in more misconception (and not reading about it)?
    c. What is the effect on users with different cultural/educational/language background?
2. How much incognito NTP message is read?
3. How much updating NTP will affect users misconceptions?

   a. Can we expand it to cover current major misconceptions?
4. How much adding contextual/inline hints[6] helps?
   a. Can we have heuristics to add inline hints for all current misconceptions?

Category two: Functionality

We can have the following additional features for incognito mode.

- Hiding traffic from network.
- Disabling/Limiting 3rd party Cookie to prevent tracking.
- Ad Blocking
- For faster browsing (by disabling some features).
- Disabling/Limiting fingerprinting surfaces including hardware/software query APIs.
- Implicitly upgrade non-secure requests to secure.
- Automatically close incognito tab after a certain amount of time of inactivity.
- Automatic suggestion of moving to incognito (temporary) mode for searches or navigations that we recognize as possibly sensitive (eg. health-related).
- Optional disabling bookmarks and other features that leave trace.

We would like to know:

1. How important each of them are for the users?
2. Should we have several browsing modes based on different user groups, or one incognito mode with selectable features?
3. Should these features be available in regular mode?

Conclusion on the Approach

Martin Shelton and I discussed the possible future steps and here is a summary:

1. Changing name and icon may have some effect on users expectation from incognito mode, but cannot solve all misconceptions. We still need user education to give a better image.
2. Although users may not want to be educated, we have to provide the means to do so.

[6] E.g. reminding users who are signing into a website that their identity will be known from this point on. (https://docs.google.com/presentation/d/1pI3qMLJzatgxAsNnBhmB6aKVVd_FkWDvvUaZeHYtGR8/edit?ts=5b8364ab#slide=id.g407b372085_36_9)

Commented [4]: We can certainly ask about interest in some of these topics in research, but I think there may still be value in improving the privacy properties of incognito with some of these features, regardless.

Commented [5]: Evaluating the importance of each possibility can help us in setting priorities.

Commented [6]: What is the exact phrasing we'll use in the study? Is now the time to decide that?

Commented [7]: I think the exact phrasing will be proposed by the UX research.

Commented [8]: We can definitely ask about interest in, or understanding of these features, but I'm not convinced that building additional functionality should be based on this kind of feedback. Many of the privacy and security features outlined here are great examples of passive functionality. That is, people don't actively need to know it's happening in order to provide the benefit. But we can still call attention to these features as a benefit of using Incognito.

Commented [9]: Having them all is great, but due to limited resources and the required sacrifices for each one, knowing the priorities would help in planning.

Commented [10]: What is the exact phrasing we'll use in the study? Is now the time to decide that?

Commented [11]: I think the exact phrasing will be proposed by the UX research.

Commented [12]: We can definitely ask about interest in, or understanding of these features, but I'm not convinced that building additional functionality should be based on this kind of feedback. Many of the privac ...

Commented [13]: Having them all is great, but due to limited resources and the required sacrifices for each ...

Commented [14]: What is the exact phrasing we'll use in the study? Is now the time to decide that?

Commented [15]: I think the exact phrasing will be proposed by the UX research.

Commented [16]: We can definitely ask about interest in, or understanding of these features, but I'm not ...

Commented [17]: Having them all is great, but due to limited resources and the required sacrifices for each ...

Commented [18]: Additional ideas for changes in functionality: ...

Commented [19]: Warning people when they sign in to a site in an incognito window ...

Commented [20]: Added first suggestion to the list, and the third one to Category 1. ...

Commented [21]: FWIW: I've proposed a new mode in the past, and it was shot down for reasons of UX ...

Commented [22]: I personally think that having two configurable modes, (regular and incognito) would be ...

3. Chrome's Incognito NTP is moderately more effective compared to other browsers, but it is probably not sufficient because we believe most users will not read it closely.
4. The most feasible approach for education seems to be inline/contextual hints on possible misconceptions, and expanding them based on future studies. Users who don't want these hints can disable them in incognito NTP. We can discuss the ideas on the messages and heuristics to activate them (go/incognito_contextual_hints) and then do a user study on how much these messages can affect users understanding and trust into the incognito mode.
5. To decide about future features, the most trustable result would be based on analysis of users use cases for incognito mode. Based on the use cases we can know what features users need, and then we can divide these features into the ones that are implementable (and assign priorities to them) and the ones that cannot be reliably implemented and we would add them to the items which require inline reminders to avoid misconceptions. Appendix 1 presents a summary of use cases, current state, and needed features.

So as the next step, we will focus on finding ways to provide appropriate contextual education for incognito mode. The user study can focus on how effective they be on different misconceptions of the users and moving them towards safe and correct use of incognito mode.
The planning for future features will not be done as part of this study. Appendix 1 provides a list of features that can be added and a prioritization on them.

Appendix 1: User Use Cases and Required Features

This appendix summarises user specified use cases for private/incognito mode, along with the needed features to provide a product that fully matches the use case.

Already covered use cases

"Hiding local activities", and ***"avoiding auto login"*** are currently fully covered and we only need higher priorities for the bugs. ***"Bypassing personalization"***, ***"shoulder surfer mode"*** , and ***"browser usage by guest users"*** are also covered, especially in guest mode.

Use cases that are not in incognito goals

Some users use incognito/private mode for ***faster browsing***, expecting disabled third party cookies, extensions, and plugins. This is not part of incognito goals, but can be a side effect and focused on as a side plan.

Hiding browsing from Google/Websites

This is not possible as once user enters a website, all actions can be recorded by the website. The only possible solution is passing a bit to the website to request anonymity, but that is conflict with incognito goal of not being distinguishable from regular mode.
We can revisit this issue if we would be willing to have a permission by user to pass such a bit to websites that declare support of this mode.

Hiding Activities from Network / Location Hiding

To do this, we need a Google proxy to hide all user activities from the network.

Anonymity from Google and Websites / Tracking prevention

We are already not passing all former credentials and cookies to Google/Websites in incognito mode, but to have complete anonymity, we need a Google proxy to cover IP addresses, have more focus on fingerprinting prevention, and have more control on 3rd party cookies.

More Security

Some users consider incognito as a more secure browsing mode. Although this is not among current promises, we can add more secure experience like an enforced HTTPS or HTTPS-first mode.

Undetectable Incognito

This is not a feature request by users, but a by-requirement of having a browsing experience that is not altered by the websites because of users' choice of more privacy. To do so, all disabled features in incognito mode should be implemented in accordance with incognito, so that they would not provide detectable behavior for the websites.

Summary (of Appendix 1)

To provide a product that works as advertised, we can put priority on solving current bugs and the ones that result in incognito detectability.
But to add more features, the most wanted features seem to be anonymity from network (which requires Google Proxy) and websites (which requires less finger printability and third party cookie blocking).
We can also plan for a more secure or faster browsing experience by adding features in that direction, including HTTPS-first/only mode and disabling extensions, third party cookies, and other possibly unnecessary modules.

PRODBEG: GOOG-CALH-00173819
PRODBEGATT:
PRODEND: GOOG-CALH-00173825
PRODENDATT:
PRODVOL: CROSS-PROD002
2nd_CROSS_BEGBATES:
2nd_CROSS_ENDBATES:
AllCustodians: Helen Harris
TO:
FROM:
CC:
BCC:
CONFIDENTIALITY: CONFIDENTIAL
CROSS_ALLCUSTODIANS:
CROSS_ATTACHMENTNAME:
CROSS_BEGATTACH:
CROSS_BEGBATES: GOOG-CABR-00552177
CROSS_CC:
CROSS_CONFIDENTIALITY:
CROSS_CUSTODIAN:
CROSS_DATECREATED:
CROSS_DATEMOD:
CROSS_DATERECEIVED:
CROSS_DATESENT:
CROSS_DE-DUPED CUSTODIANS:
CROSS_ENDATTACH:
CROSS_ENDBATES: GOOG-CABR-00552183
CROSS_FILEEXTENSION:
CROSS_FILENAME:
CROSS_FROM:
CROSS_MD5 HASH:
CROSS_MESSAGE ID:
CROSS_OWNER:
CROSS_PRODVAL:
CROSS_REDACTED:
CROSS_SUBJECT:
CROSS_TITLE:
CROSS_TO:
CUSTODIAN/SOURCE: Helen Harris
DATECREATED: 08/09/2018
DATELASTMOD: 11/21/2018
DATERCVD:
DATESENT:
DeDupedCustodians: Helen Harris
DOCEXT: docx
FILENAME: 2- Incognito User Study Questions_1V9vgva9qAJGl-uI-o_Rnb9tOXCzL8fG1KEK--Qkg_umM.docx
ILS_ProdDate: 09/01/2021
CROSS_ILS_ProdDate: 09/01/2021
MD5 HASH: 60EFBF48B1C1C1C4191A81475DA22658
MessageID:
NATIVEFILE:
Owner: rhalavati@google.com
PAGES: 7
REDACTED: N

SUBJECT: